STATE OF ALABAMA

Information Technology Standard

Standard 670-03S1: Vulnerability Management

1. INTRODUCTION:

Timely patching of security vulnerabilities is critical to maintaining the operational availability, confidentiality, and integrity of information technology (IT) systems. Vulnerability management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities through a systematic, accountable, and documented process for managing the timely deployment of patches and other threat remediation practices.

2. OBJECTIVE:

To maintain a consistently configured environment, secure against known vulnerabilities in operating system and application software, using a managed remediation process.

3. SCOPE:

These requirements apply to all administrators and managers of State-managed information system resources.

4. REQUIREMENTS:

4.1 VULNERABILITY MANAGEMENT PROGRAMS

> *Policy: IT Managers shall create, or participate in, a comprehensive, documented, and accountable process for identifying and addressing vulnerabilities, threats, and remediation within their area of responsibility.*

In accordance with the recommendations of the National Institute of Standards and Technology (NIST) found in Special Publication 800-40: Creating a Patch and Vulnerability Management Program, State of Alabama vulnerability management programs shall implement the following tasks:

- Create an inventory of all information technology assets
- Create a patch and vulnerability group (recommended)
- Continuously monitor for vulnerabilities and threats using automated and manual methods
- Prioritize patch application; use phased deployments as appropriate
- Test patches before deployment
- Deploy enterprise-wide automated patch management solutions whenever possible
- Create a remediation database (see Definitions)
- Use automatically updating applications as appropriate

- Verify vulnerabilities have been remediated
- Train applicable staff on vulnerability monitoring and remediation techniques

4.2 SECURE SYSTEMS CONFIGURATION

Policy: System/Network Administrators shall maintain secure systems in accordance with the organizational vulnerability management program.

System/Network Administrators shall ensure secure system configurations to include all pertinent patches and fixes by routinely reviewing vendor sites, bulletins, and notifications and proactively updating systems with fixes, patches, definitions, service packs, or implementation of vulnerability mitigation strategies in accordance with the organizational vulnerability management program.

5. ADDITIONAL INFORMATION:

5.1 POLICY

Information Technology Policy 670-03: Vulnerability Management
http://isd.alabama.gov/policy/Policy_670-03_Vulnerability_Management.pdf

5.2 RELATED DOCUMENTS

Information Technology Dictionary
http://isd.alabama.gov/policy/IT_Dictionary.pdf

Signed by Art Bess, Assistant Director

6. DOCUMENT HISTORY:

Version	Release Date	Comments
Original	12/12/2006	